512.74
B73b

-aun, W

THE UNIVERSITY
OF ILLINOIS
LIBRARY
512.~~814~~ 74
B73b

UNIVERSITY OF
ILLINOIS LIBRARY
AT URBANA-CHAMPAIGN
MATHEMATICS

Bestimmung der Körperdiskriminante in einem kubischen Zahlkörper.

UNIVERSITY LIBRARY
UNIVERSITY OF ILLINOIS
URBANA

Inaugural-Dissertation

der

mathematischen und naturwissenschaftlichen Fakultät

der

Kaiser Wilhelms-Universität zu Strassburg

zur Erlangung der Doktorwürde

vorgelegt von

Wanda Braun

aus Strassburg i. E.

STRASSBURG i. E.

Els.-Lothr. Druckerei, Abteilung C. Müh & Cie., Kinderspielgasse 20.

1909.

Gedruckt mit Genehmigung der mathematischen und naturwissenschaftlichen Fakultät Strassburg.

Referent: Prof. Dr. H. Weber.

74
512.814
B73b

Einteilung.

Mathematics Research 22Ap'14 Stechert 45 1Se'14 GRACE BARNES

264797

Einleitung.

Das Problem der Bestimmung der Diskriminante des kubischen Körpers ist zum ersten Male von Woronoj behandelt worden in der Abhandlung: „Über die ganzen algebraischen Zahlen, die von einer Wurzel der Gleichung dritten Grades abhängen.“ St. Petersburg 1894. Durch die Auflösung der Kongruenz $\varsigma^3 - r\varsigma - s \equiv 0 \pmod{p}$ findet er die Minimalbasis $\omega_1, \omega_2, \omega_3$ und daraus die Körperdiskriminante. In der vorliegenden Arbeit wird nun die Körperdiskriminante direkt bestimmt. Es wird der Satz benutzt, dass die Körperdiskriminante stets ein Teiler der Diskriminante der Gleichung ist, die den Körper definiert und sich von dieser Gleichungsdiskriminante nur um einen quadratischen Faktor unterscheidet, und es wird untersucht, ob eine Primzahl p in diesem Faktor aufgeht oder nicht. Im ersten Teile werden die zur Verwendung kommenden fundamentalen Begriffe der Theorie des algebraischen Zahlkörpers dargestellt und zwar in der Gestalt, wie sie Prof. Weber im 2. Bande der Algebra (IV. Buch) gegeben hat. Hieran schliesst sich die Bestimmung der Diskriminante des quadratischen Zahlkörpers von Dedekind.

ERSTER TEIL.

Zusammenstellung der zu Grunde liegenden Prinzipien.

I. Die algebraische Zahl und die Zahlkörper.

Eine Zahl Θ, die einer rationalen Gleichung

$$(1) \quad f(\Theta) = \Theta^n + a_1 \Theta^{n-1} + \ldots\ldots a_n = 0$$

genügt, heisst eine algebraische Zahl. Ist n der Grad dieser Gleichung, so heisst n der Grad von Θ. Es wird vorausgesetzt, dass $f(\Theta)$ die Gleichung niedrigsten Grades bezeichnet, der Θ genügt, dass also $f(\Theta)$ irreduzibel sei, d. h. dass es keine Doppelwurzel besitzt und deshalb die Gleichungsdiskriminante nicht verschwindet. Sind die Koeffizienten der Gleichung (1), $a_1\, a_2 \ldots . a_n$ ganze rationale Zahlen, so ist Θ eine ganze algebraische Zahl. Über die ganzen algebraischen Zahlen gelten die folgenden Sätze [1]:

α) Eine ganze algebraische Zahl, die zugleich rational ist, ist notwendig eine ganze rationale Zahl.

β) Summe, Differenz und Produkt zweier ganzer Zahlen sind wieder ganze Zahlen;

γ) Jede algebraische Zahl Θ lässt sich durch Multiplikation mit einer natürlichen Zahl in eine ganze algebraische Zahl verwandeln.

Die Theorie der algebraischen Zahlen stützt sich auf den fundamentalen Begriff des Zahlkörpers. Ein

---

[1]) Weber, Algebra, 2. Band, IV. Buch, § 149.

UNIVERSITY OF ILLINOIS LIBRARY URBANA

System von Zahlen wird ein Zahlkörper genannt, wenn es so in sich vollendet und abgeschlossen ist, dass die vier fundamentalen Rechenoperationen, die Addition, die Subtraktion, die Multiplikation und die Division, ausgeführt mit irgend welchen Zahlen des Systems, ausgenommen die Division durch Null, immer auf Zahlen führen, die demselben System angehören [2]). Sind die Zahlen des Körpers algebraische Zahlen, so heisst der Körper ein algebraischer Zahlkörper $\Omega(\theta)$. θ heisst die den Körper definierende Zahl, ihr Grad der Grad des Körpers. Der einzige Körper ersten Grades ist der Körper der rationalen Zahlen. Alle übrigen Körper enthalten diesen Körper als Teiler. Ist n der Grad von θ, so heissen $\theta', \theta'' \ldots \theta^{(n-1)}$ die zu θ konjugierten Zahlen. Jede Zahl des Körpers lässt sich eindeutig in der Form darstellen:

$$\omega = h_1 + h_2\theta + h_3\theta^2 + \ldots h_n\theta^{n-1}$$

wo die $h_1, h_2 \ldots h_n$ rationale Zahlen sind. Die zu ω konjugierten Zahlen sind:

$$\omega' = h_1 + h_2\theta' + h_3\theta'^2 + \ldots h_n\theta'^{(n-1)}$$
$$\omega'' = h_1 + h_2\theta'' + h_3\theta''^2 + \ldots h_n\theta''^{(n-1)}$$
$$\vdots$$
$$\omega^{(n-1)} = h_1 + h_2\theta^{(n-1)} + h_3\theta^{(n-1)^2} + \ldots h_n\theta^{(n-1)^{n-1}}$$

Eine symmetrische Funktion der konjugierten Zahlen ist eine rationale Zahl. Unter den symmetrischen Funktionen sind zwei von besonderer Wichtigkeit, die Summe und das Produkt, von denen die erste die Spur, die zweite die Norm genannt wird. Man bezeichnet die beiden Zahlen durch $S(\theta)$ und $N(\theta)$.

$$S(\theta) = \theta + \theta' + \theta'' + \ldots \theta^{(n-1)} = -a_1$$
$$N(\theta) = \theta \cdot \theta' \cdot \theta'' \ldots \theta^{(n-1)} = (-1)^n a_n.$$

[2]) Weber, Algebra, 1. Band, 3. Buch, § 146.

Über die Spur und die Norm gelten folgende Sätze:

α) Die Summe oder Differenz zweier Spuren ist gleich der Spur der Summe oder Differenz

$$S(\omega_1) \pm S(\omega_2) = S(\omega_1 + \omega_2);$$

β) Das Produkt zweier Normen ist gleich der Norm des Produktes

$$N(\omega_1) . N(\omega_2) = N(\omega_1 . \omega_2)$$

Ganz ähnliche Sätze gelten offenbar auch für die Quotienten. Wenn ω eine rationale Zahl ist, so sind die n konjugierten Zahlen mit ω identisch, und es ist daher

$$S(\omega) = n . \omega$$
$$N(\omega) = \omega^n$$

2. Basis eines algebraischen Zahlkörpers. Diskriminanten [3].

Es sei

$$(1) \quad f(\Theta) = \Theta^n + a_1 \Theta^{n-1} + \dots a^n = 0$$

die irreduzible Gleichung n^{ten} Grades, die den algebraischen Körper $\Omega(\Theta)$ definiert. Der Körper Ω ist dann der Inbegriff aller Zahlen von der Form

$$(2) \quad \omega = h_1 + h_2 \Theta + h_3 \Theta^2 + \dots h_n \Theta^{n-1},$$

worin $h_1, h_2 \dots h_n$ rationale Zahlen sind. Die Zahl 0, die dem Körper auch angehört, ist nur dann in der Form (2) enthalten, wenn

$$h_1 = h_2 = h_3 = \dots h_n = 0$$

ist. Da die Gleichung

$$h_1 + h_2 \Theta + \dots h_n \Theta^{n-1} = 0$$

nur bestehen kann, wenn alle $h_i = 0$ sind, so heissen die n Zahlen $1, \Theta, \Theta^2 \dots \Theta^{n-1}$ voneinander linear unabhängig. Betrachten wir ein beliebiges System von n Zahlen

[3]) Weber, Algebra II. 4, § 161.

$$(3)\quad \begin{aligned} \omega_1 &= h_{11} + h_{21}\Theta + \dots h_{n1}\Theta^{n-1} \\ \omega_2 &= h_{12} + h_{22}\Theta + \dots h_{n2}\Theta^{n-1} \\ &\vdots \\ \omega_n &= h_{1n} + h_{2n}\Theta + \dots h_{nn}\Theta^{n-1} \end{aligned}$$

so sind die n Zahlen $\omega_1, \omega_2, \omega_3 \dots \omega_n$ nur dann voneinander linear unabhängig, wenn die Determinante

$$(4)\qquad H = \begin{vmatrix} h_{11} & h_{21} \dots h_{n1} \\ h_{12} & h_{22} \dots h_{n2} \\ \vdots & \\ h_{1n} & h_{2n} \dots h_{nn} \end{vmatrix}$$

von Null verschieden ist. Eliminieren wir aus den Gleichungen (2) und (3) die Potenzen von Θ, so ergibt sich eine Beziehung von der Form

$$(5)\qquad \omega = k_1\omega_1 + k_2\omega_2 + \dots k_n\omega_n$$

In dieser Form kann man also jede Zahl des Körpers darstellen. Ein solches System von Zahlen wie

$$\omega_1 \quad \omega_2 \dots \omega_n$$

nennt man eine Basis des Körpers. Eine solche Basis bilden auch die Potenzen von Θ.

Bezeichnet man mit $\omega_{r1}, \omega_{r2} \dots \omega_{rn}$ die mit ω_r konjugierten Zahlen, so ist das Determinantenquadrat

$$\begin{vmatrix} \omega_{11} & \omega_{12} \dots \omega_{1n} \\ \omega_{21} & \omega_{22} \dots \omega_{2n} \\ \vdots & \vdots \\ \omega_{n1} & \omega_{n2} \dots \omega_{nn} \end{vmatrix}^2 = \Delta(\omega_1\,\omega_2 \dots \omega_n)$$

eine symmetrische Funktion der konjugierten Werte $\Theta_1, \Theta_2 \dots \Theta_n$ und ist folglich eine rationale Zahl. Diese Zahl heisst die Diskriminante des Systems

$\omega_1, \omega_2, \ldots . \omega_n$. So ist die Diskriminante des Systems $(1, \Theta, \Theta^2 \ldots . \Theta^{n-1})$

$$\Delta(1, \Theta, \Theta^2, \ldots . \Theta^{n-1}) = \begin{vmatrix} 1 & \Theta_1 \ldots . \Theta_1^{n-1} \\ 1 & \Theta_2 \ldots . \Theta_2^{n-1} \\ \vdots & \vdots \quad\quad \vdots \\ 1 & \Theta_n \ldots . \Theta_n^{n-1} \end{vmatrix}^2$$

gleich der Diskriminante der Gleichung

$$f(\Theta) = \Theta^n + a_1 \Theta^{n-1} + \ldots . a_n = 0$$

Diese Zahl ist also sicher wegen der Irreduzibilität von $f(\Theta)$ von Null verschieden.

Nun ist nach dem Multiplikationssatz der Determinanten, wenn man (3) und (4) berücksichtigt

$$\begin{vmatrix} \omega_{11} & \omega_{12} \ldots \omega_{1n} \\ \omega_{21} & \omega_{22} \ldots \omega_{2n} \\ \vdots & \vdots \\ \omega_{n1} & \omega_{n2} \ldots \omega_{nn} \end{vmatrix}^2 = \begin{vmatrix} h_{11} & h_{12} \ldots h_{1n} \\ h_{21} & h_{22} \ldots h_{2n} \\ \vdots & \vdots \quad\quad \vdots \\ h_{n1} & h_{n2} \ldots h_{nn} \end{vmatrix}^2 \cdot \begin{vmatrix} 1 & \Theta \ldots \Theta_{n-1} \\ 1 & \Theta_1 \ldots \Theta_1^{n-1} \\ \vdots & \vdots \quad\quad \vdots \\ 1 & \Theta_n \ldots \Theta_n^{n-1} \end{vmatrix}^2$$

also

$$\Delta(\omega_1 \, \omega_2 \ldots \omega_n) = H^2 \Delta(1, \Theta, \ldots \Theta^{n-1})$$

Hieraus folgt: 1) dass die Diskriminante einer Basis immer von Null verschieden ist; 2) dass die Diskriminante aller Basen des Körpers stets dasselbe Vorzeichen haben; 3) dass, da H eine rationale Zahl ist, das Verhältnis der Diskriminanten verschiedener Basen des Körpers das Quadrat einer rationalen Zahl ist; 4) dass irgend ein System von n Zahlen des Körpers immer dann eine Basis des Körpers ist, wenn das Determinantenquadrat H^2 nicht verschwindet.

3. Die Minimalbasis und die Körperdiskriminante [4].

Ist

$$\omega_1, \omega_2, \ldots . \omega_n$$

eine Basis des Körpers, so ist

$$c_1 \omega_1, c_2 \omega_2 \ldots . c_n \omega_n$$

auch eine Basis, denn es ist

$$\Delta (c_1 \omega_1, c_2 \omega_2 \ldots c_n \omega_n) = c_1^2 c_2^2 \ldots c_n^2 . \Delta (\omega_1 \omega_2 \ldots \omega_n)$$

Da nun jede algebraische Zahl durch Multiplikation mit einer rationalen Zahl in eine ganze rationale Zahl verwandelt werden kann, so gibt es also Basen in Ω, deren Elemente lauter ganze Zahlen sind. Die Diskriminante einer solchen Basis ist eine ganze rationale Zahl, die von Null verschieden ist. Diese Zahl ändert sich, wenn eine andere ganzzahlige Basis gewählt wird. Sie behält aber für denselben Körper dasselbe Vorzeichen.

Es leuchtet nun ein, dass unter allen Basen des Körpers, welche aus lauter ganzen Zahlen bestehen und deren Diskriminanten folglich ganze rationale, von Null verschiedene Zahlen sind, auch mindestens eine solche Basis existieren muss, deren Diskriminante Δ, absolut genommen, ein Minimum ist. Diese kleinste Diskriminante Δ heisst die Körperdiskriminante oder auch wegen ihrer grossen Wichtigkeit die Grundzahl des Körpers Ω. Es gibt immer eine aus ganzen Zahlen

$$\omega_1 \omega_2 \ldots . \omega_n$$

bestehende Basis von Ω, deren Diskriminante $= \Delta$ ist. Eine solche Basis heisst eine Minimalbasis.

Die grosse Wichtigkeit der Minimalbasis und der Körperdiskriminante ergibt sich sofort aus folgendem Satz:

---

[4]) Weber, Algebra II. 4, § 162.

„Wenn $\omega_1\ \omega_2 \ldots \omega_n$

eine Minimalbasis ist, so sind in der Form

$$(2) \qquad \omega = k_1 \omega_1 + k_2 \omega_2 + \ldots k_n \omega_n$$

alle ganzen Zahlen des Körpers Ω enthalten, wo $k_1, k_2 \ldots k_n$ ganze rationale Zahlen sind."

Beweis: Da $\omega_1, \omega_2 \ldots \omega_n$ eine Basis des Körpers ist, so können alle Zahlen in der Form (2) dargestellt werden, wenn man für die $k_1\ k_2 \ldots k_n$ rationale Brüche zulässt. Wir nehmen an, es sei eine ganze Zahl in der Form darstellbar

$$(3) \qquad \omega = \frac{k_1 \omega_1 + k_2 \omega_2 + \ldots k_n \omega_n}{k}$$

worin $k_1, k_2 \ldots k_n$ ganze rationale Zahlen sind, die nicht alle mit k denselben gemeinsamen Teiler haben. Man kann k auch als eine Primzahl annehmen, durch die nicht alle $k_1, k_2 \ldots k_n$ teilbar sind. Es sei $k = p\,k'$ und k_1 sei durch p nicht teilbar; dann lässt sich die ganze rationale Zahl l so bestimmen, dass

$$l\,k_1 \equiv 1 \pmod{p}$$

wird. Es folgt dann aus (3)

$$(4) \qquad l\,k'\,\omega - \frac{l\,.\,k_1 - 1}{p}\,\omega_1 =$$

$$\frac{\omega_1 + l\,k_2\,\omega_2 + \ldots l\,k_n\,\omega_n}{p} = \omega_1'$$

und ω_1' ist ebenfalls eine ganze algebraische Zahl. Setzen wir

$$(5) \qquad \begin{aligned} \omega_2' &= \omega_2 \\ &\vdots \\ \omega_n' &= \omega_n\,, \end{aligned}$$

so bilden die Zahlen

$$\omega_1',\ \omega_2' \ldots \omega_n'$$

eine ganzzahlige Basis von Ω, weil sich alle Zahlen ω linear durch $\omega_1', \omega_2' \ldots \omega_n'$ ausdrücken lassen. Dann folgt:

$$(6) \quad \Delta(\omega_1' \; \omega_2 \ldots . \omega_n') = \frac{1}{p^2} \Delta(\omega_1, \omega_2, \ldots . \omega_n)$$

Die Diskriminante $\Delta(\omega_1', \omega_2' \ldots .. \omega_n')$ ist also kleiner als $\Delta(\omega_1, \omega_2 \ldots . \omega_n)$. Dies widerspricht der Annahme, dass $\omega_1, \omega_2 \ldots . \omega_n$ eine Minimalbasis sei. Damit ist der Satz bewiesen.

Wie wichtig die Körperdiskriminante für die Theorie der algebraischen Zahlen ist, will ich noch durch Anführen einiger Sätze andeuten. So hat Dedekind den Satz bewiesen: Die Diskriminante des Zahlkörpers enthält alle und nur diejenigen Primzahlen als Faktoren, welche durch das Quadrat eines Primideals teilbar sind.

Wie Minkowsky gezeigt hat, besteht der für die Bestimmung der Klassenanzahl fundamentale Satz: „In jeder Idealklasse gibt es ein Ideal, dessen Norm die absolut genommene Quadratwurzel aus der Körperdiskriminante nicht übersteigt.“ Um die Klassenanzahl mittels dieses Satzes zu bestimmen, braucht man nur alle Ideale des vorgelegten Körpers in Betracht zu ziehen, deren Normen $\overline{\gtreqless} \sqrt{\Delta}$ sind und die unter ihnen vorhandenen Äquivalenzen bestimmen.

Ist Δ die Körperdiskriminante, Θ die den Körper definierende Zahl, D die Gleichungsdiskriminante, so ist, wenn D keinen Quadratfaktor enthält, $D = \Delta$. Wenn aber D einen Quadratfaktor enthält, dann bietet die Bestimmung einer Minimalbasis und der Körperdiskriminante in dem allgemeinen Fall grosse Schwierigkeit. In dem Falle des quadratischen Zahlkörpers ist die Bestimmung noch ziemlich einfach. Ich führe in folgendem diese Bestimmung durch, wie sie Dedekind gegeben hat, um dann zu meiner Aufgabe, der Bestimmung der Körperdiskriminante im kubischen Zahlkörper, zu kommen.

ZWEITER TEIL.

Bestimmung der Körperdiskriminante im quadratischen Zahlkörper[5].

Der quadratische Zahlkörper wird definiert durch die Gleichung

$$(1) \quad x^2 + a x + b = 0$$

Die Wurzel Θ dieser Gleichung ist

$$(2) \quad \Theta = \frac{- a + \sqrt{a^2 - 4 b}}{2}$$

Setzt man

$$\sqrt{a^2 - 4 b} = \beta \sqrt{d}$$

wo d keinen quadratischen Faktor enthält und auch nicht gleich + 1 ist, so lässt sich jede Wurzel der Gleichung (1) in der Form darstellen

$$(3) \quad \Theta = r + s \sqrt{d},$$

wo r und s rationale Zahlen sind, von denen die letztere nicht verschwindet. Alle Zahlen des quadratischen Körpers sind dann von der Form

$$\omega = \alpha + \beta \Theta = t + u \sqrt{d} = \frac{x + y \sqrt{D}}{z},$$

wo x, y, z ganze rationale Zahlen ohne gemeinsamen Teiler bedeuten, von denen die letzte z positiv ist.

[5]) Dirichlet-Dedekind, Zahlentheorie. Supplement XI.

Soll nun ω eine ganze Zahl sein, so muss auch die konjugierte Zahl

$$\omega' = \frac{x - y\sqrt{d}}{z}$$

ganz sein, also auch

$$\omega + \omega' = \frac{2x}{z} \quad \text{und}$$

$$\omega \,.\, \omega' = \frac{x^2 - dy^2}{z^2}$$

und umgekehrt: Ist dies der Fall, so ist ω als Wurzel der Gleichung

$$\omega^2 - \frac{2x}{z}\omega + \frac{x^2 - dy^2}{z^2} = 0$$

eine ganze Zahl. Enthält z eine Primzahl $p > 2$ als Faktor, so muss auch x diesen Faktor p enthalten; ferner muss dann p^2 in $x^2 - dy^2$ aufgehen, und da p^2 in x^2 enthalten ist, d aber keinen quadratischen Faktor enthält, muss y durch p teilbar sein. Wären x und z durch 2 teilbar, so würde ebenso folgen, dass y durch 2 teilbar sein müsste. Dies widerspricht aber der Voraussetzung, dass x, y, z ohne gemeinschaftlichen Teiler sind, also muss $p = 1$ sein. Da nun z und x relative Primzahlen sind und z in 2x aufgeht, muss $z = 1$ oder $z = 2$ sein. Es ist noch zu untersuchen, wann der zweite Fall möglich ist. Ist $z = 2$, so ist x ungerade, also $x^2 \equiv 1 \pmod 4$; da ferner $x^2 - dy^2$ durch $z^2 = 4$ teilbar ist, so ist $dy^2 \equiv 1 \pmod 4$; also sind d und y ungerade, also auch

$$y^2 \equiv 1 \pmod 4$$
$$d \equiv 1 \pmod 4$$

Diese letzte Bedingung ist erforderlich, damit der Fall $z = 2$ eintreten kann; und umgekehrt, wenn $d \equiv 1 \pmod 4$, so ist jede Zahl

$$\frac{x + y\sqrt{d}}{2},$$

in welcher x, y beide ungerade sind, ganz. Da zu diesen Zahlen noch alle diejenigen hinzukommen, in welchen $z = 1$ ist, so besteht das System aller ganzen Zahlen des Körpers in diesem Falle aus allen Zahlen von der Form

$$x + y\,\frac{1 + \sqrt{d}}{2}.$$

Die Minimalbasis ist also in diesem Fall

$$1 \qquad \frac{1 + \sqrt{d}}{2}$$

und die Körperdiskriminante

$$\Delta = \begin{vmatrix} 1 & \dfrac{1 + \sqrt{d}}{2} \\ 1 & \dfrac{1 - \sqrt{d}}{2} \end{vmatrix}^2 = d$$

Ist aber $d \equiv 3$, oder $d \equiv 2 \pmod 4$, so muss $z = 1$ sein, alle Zahlen des Körpers sind von der Form

$$x + y\sqrt{d}.$$

Die Minimalbasis ist in diesem Fall

$$1, \quad \sqrt{d}$$

und die Körperdiskriminante

$$\Delta = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d$$

Die Körperdiskriminante Δ im quadratischen Körper ist also durch folgendes einfache Resultat bestimmt:

Ist

$$d \equiv 1 \pmod 4)$$

so ist

$$\Delta = d\,.$$

Ist

$$d \equiv 2,\ \text{oder}\ d \equiv 3 \pmod 4)$$

so ist

$$\Delta = 4\,d\,,$$

wo d das Produkt aller in der Gleichungsdiskriminante $a^2 - 4\,b$ nur zur ersten Potenz aufgehenden Primfaktoren ist.

DRITTER TEIL.

Bestimmung der Körperdiskriminante in einem kubischen Zahlkörper.

I. Woronojs Methode zur Bestimmung der Minimalbasis und der Körperdiskriminante [6]).

Woronoj gründet seine Methode auf die Auflösung der Kongruenz

$$\Theta^3 - z\,\Theta - x \equiv 0 \pmod{p}$$

Er kommt zu folgendem Resultat: Alle ganzen Zahlen, die von einer Wurzel der irreduzibeln Gleichung

$$\Theta^3 - z\,\Theta - x = 0$$

abhängig sind, sind darstellbar in der Form

$$(1)\quad A + A' \frac{-\xi + \Theta}{\delta} + A'' \frac{\xi^2 - z + \xi\,\Theta + \Theta^2}{\delta^2\,\sigma}$$

A, A′, A″ sind willkürliche ganze rationale Zahlen. ξ ist die gemeinsame Lösung der beiden Kongruenzen

$$\xi^3 - z\,\xi - x \equiv 0 \pmod{\delta^3\,\sigma^2}$$
$$3\,\xi^2 - z \equiv 0 \pmod{\delta^2\,\sigma}$$

σ ist die grösste ganze Zahl, für welche diese Kongruenzen

[6]) Woronoj: „Über die ganzen algebraischen Zahlen, die von einer Wurzel der Gleichung dritten Grades abhängen. In russischer Sprache erschienen in St. Petersburg, 1894.

gleichzeitig möglich sind. Ist d die grösste ganze Zahl für welche die Kongruenzen

$$z \equiv 0 \pmod{d^2}$$
$$x \equiv 0 \pmod{d^3}$$

möglich sind, so ist $\delta = 3\,d$ oder $\delta = d$, je nachdem die Kongruenzen

$$\frac{z}{d^2} \equiv 3 \pmod 9$$

$$\frac{x}{d^3} \equiv \pm \left(1 + \frac{z}{d^2}\right) \pmod{27}$$

lösbar sind oder nicht. In der Woronoj'schen Abhandlung werden die Grössen δ, σ, ξ gefunden und bewiesen, dass alle ganzen Zahlen in der Form (1) darstellbar sind, die Minimalbasis ist

$$1, \quad \frac{-\xi + \theta}{\delta}, \quad \frac{\xi^2 - z + \xi\theta + \theta^2}{\delta^2\sigma}$$

und die Körperdiskriminante stellt sich in der Form dar

$$(2) \qquad \Delta = \begin{vmatrix} 1 & \dfrac{-\xi + \theta}{\delta}, & \dfrac{\xi^2 - z + \xi\theta + \theta^2}{\delta^2\sigma} \\ 1 & \dfrac{-\xi + \theta'}{\delta}, & \dfrac{\xi^2 - z + \xi\theta' + \theta'^2}{\delta^2\sigma} \\ 1 & \dfrac{-\xi + \theta''}{\delta}, & \dfrac{\xi^2 - z + \xi\theta'' + \theta''^2}{\delta^2\sigma} \end{vmatrix}^2$$

$$= \frac{1}{\delta^6\sigma^2} \begin{vmatrix} 1 & \theta & \theta^2 \\ 1 & \theta' & \theta'^2 \\ 1 & \theta'' & \theta''^2 \end{vmatrix} = \frac{1}{\delta^6\sigma^2}\,D$$

Ist z. B. der Körper definiert durch die Gleichung

$$\theta^3 + 33\,\theta - 47 = 0,$$

so ist die Gleichungsdiskriminante $D = -3^8 \,.\, 31$.

Die Kongruenzen

$$-33 \equiv 0 \pmod{d^3}$$
$$47 \equiv 0 \pmod{d^2}$$

haben die gemeinsame Lösung $d = 1$.

Nun ist

$$-33 \equiv 3 \pmod 9$$
$$47 \equiv -(1 + 33) \pmod{27}$$

Also ist $\delta = 3$

Da nach (2) D durch $\delta^6 = 3^6$ teilbar ist, kann σ, da es quadratischer Faktor von D ist, nur noch $= 1$ oder $= 3$ sein.

Die Kongruenzen

$$\Theta^3 + 33\,\Theta - 47 \equiv 0 \pmod{3^3 \cdot 3}$$
$$3\,\Theta^2 + 33 \equiv 0 \pmod{3^2 \cdot 3}$$

haben die gemeinsame Lösung

$$\xi \equiv -4 \pmod 9$$

Also ist $\sigma = 3$ und die

Körperdiskriminante

$$\Delta = \frac{1}{\delta^6\,\sigma^2} D = \frac{1}{3^6 \cdot 3^2} \cdot 3^8 \cdot 31 = 31$$

2. Der kubische Zahlkörper.

Der kubische Körper ist definiert durch die Gleichung

$$(1) \quad \Theta^3 + A_1\,\Theta^2 + A_2\,\Theta + A_3 = 0$$

Da aber jede kubische Gleichung auf die Form gebracht werden kann:

$$(2) \quad \Theta^3 - z\,\Theta - x = 0 \quad ,$$

kann jeder kubische Körper durch eine Gleichung (2) definiert werden.

Wir bilden die Diskriminante dieser Gleichung.

Es ist
$$\Theta^3 = x\,\Theta + x$$
$$S(\Theta) = 0$$
$$S(\Theta^3) = 3\,x + z\,S(\Theta) = 3\,x$$
$$\Theta(\Theta^2 - z) = x$$
$$\Theta^2(\Theta^2 - z)^2 = x^2$$
$$\Theta^2 = \sigma$$
$$\sigma(\sigma - z)^2 = x^2$$
$$\sigma^3 - 2\,\sigma^2 z + \sigma z^2 - x^2 = 0$$
$$S(\Theta^2) = 2\,z$$
$$\Theta^4 = \Theta\,.\,x + \Theta^2 z$$
$$S(\Theta^4) = z\,.\,S(\Theta^2) = 2\,z^2$$

Die Diskriminante von (2) ist

$$D(1,\ \Theta,\ \Theta^2) = \begin{vmatrix} 1 & \Theta & \Theta^2 \\ 1 & \Theta_1 & \Theta_1{}^2 \\ 1 & \Theta_2 & \Theta_2{}^2 \end{vmatrix}^2 =$$

$$\begin{vmatrix} S(1), & S(\Theta), & S(\Theta^2) \\ S(\Theta), & S(\Theta^2), & S(\Theta^3) \\ S(\Theta^2), & S(\Theta^3), & S(\Theta^4) \end{vmatrix} = \begin{vmatrix} 3 & 0 & 2\,z \\ 0 & 2\,z & 3\,x \\ 2\,z & 3\,x & 2\,z^2 \end{vmatrix}$$
$$= 4\,z^3 - 27\,x^2$$

Wir zerlegen nun die Diskriminante D in quadratische und lineare Faktoren.

$$(3) \quad D = y^2\,.\,\mathfrak{D}$$

y^2 ist die grösste in D enthaltene Quadratzahl.

Die Diskriminante D der kubischen Gleichung ist, wie im ersten Teil gezeigt worden ist, durch die Körperdiskriminante Δ teilbar, und der Quotient ist ein Quadrat.

$$(4) \quad y^2\,.\,\mathfrak{D} = \varkappa^2\,\Delta$$

$\mathfrak{D}$ ist durch kein Quadrat teilbar. Also muss Δ durch $\mathfrak{D}$ teilbar sein, und der Quotient ist wieder ein Quadrat.

$$(5) \quad \Delta = \lambda^2\,.\,\mathfrak{D} \qquad \text{also}$$
$$(6) \quad y^2 = \varkappa^2\,.\,\lambda^2$$

Es kommt alles darauf an, λ zu bestimmen. Wir werden also untersuchen, wann die Primzahl p, wenn sie in y aufgeht, in λ enthalten ist und wann nicht. Wir unterscheiden dabei folgende Fälle:

1) $p > 3$
2) $p = 2$
3) $p = 3$

Da wir in den folgenden Ausführungen öfters zu bestimmen haben werden, wann eine Zahl

$$\eta = \alpha + \beta\,\Theta + \gamma\,\Theta^2$$

algebraisch ganz ist, und zu diesem Zwecke untersuchen müssen, ob die Koeffizienten der Gleichung, der diese Zahl genügt, rational ganz sind, so wollen wir hier gleich die Gleichung bestimmen, deren Wurzel die Zahl

$$\eta = \alpha + \beta\,\Theta + \gamma\,\Theta^2$$

ist. Wir setzen

$$\begin{aligned} \eta &= \alpha + \beta\,\Theta + \gamma\,\Theta^2 \\ \eta\,\Theta &= \gamma\,x + (\alpha + \gamma\,z)\,\Theta + \beta\,\Theta^2 \\ \eta\,\Theta^2 &= \beta\,x + (\gamma\,x + \beta\,z)\,\Theta + (\alpha + \gamma\,z)\,\Theta^2 \end{aligned}$$

$$-f(\eta) = \begin{vmatrix} \alpha - \eta & \beta & \gamma \\ \gamma\,x & \alpha + \gamma\,z - \eta & \beta \\ \beta\,x & \gamma\,x + \beta\,z & \alpha + \gamma\,z - \eta \end{vmatrix} = 0$$

$$f(\eta) = \eta^3 - A_1\,\eta^2 + A_2\,\eta - A_3 = 0$$

$$f(\eta) = f(0) + \eta\,f'(0)$$

$$\begin{aligned} A_1 &= 3\,\alpha + 2\,\gamma\,z \\ (7) \qquad A_2 &= f'(0) \\ A^3 &= f(0) \end{aligned}$$

$$(8)\; A_2 = f'(0) = \begin{vmatrix} \alpha + \gamma\,z, & \beta \\ \gamma\,x + \beta\,z, & \alpha + \gamma\,z \end{vmatrix} + \begin{vmatrix} \alpha & \gamma \\ \beta\,x & \alpha + \gamma\,z \end{vmatrix}$$

$$+ \begin{vmatrix} \alpha & \beta \\ \gamma\,x & \alpha + \gamma\,z \end{vmatrix} = \begin{vmatrix} 3\,\alpha + \gamma\,z, & \beta \\ 3\,\gamma\,x + \beta\,z, & \alpha + \gamma\,z \end{vmatrix}$$

$$(9) \qquad A_3 = \begin{vmatrix} \alpha & \beta & \gamma \\ \gamma x & \alpha + \gamma z & \beta \\ \beta x & \gamma x + \beta z & \alpha + \gamma z \end{vmatrix}$$

Wir gehen nun zu dem ersten Teil unserer Untersuchungen über, zu dem Fall, wo die Gleichungsdiskriminante teilbar ist durch die Primzahl $p > 3$.

3. Die Primzahl $p > 3$.

Wir unterscheiden

I. x nicht teilbar durch p

II. x teilbar durch p

$$\theta^3 - z\,\theta - x = 0$$

I. Geht ein Primteiler p von $D = y^2 \mathfrak{D}$ nicht in x auf, so ist 3 z quadratischer Rest von p, denn es ist

$$4 z^3 - 27 x^2 = y^2 . \mathfrak{D}$$

$$z (2 z)^2 - 3 (3 x)^2 = y^2 . \mathfrak{D}$$

$$(2) \qquad z - 3 \left(\frac{3 x}{2 z}\right)^2 = \frac{y^2 . \mathfrak{D}}{(2 z)^2}$$

oder

$$3 z (2 z)^2 - (9 x)^2 = 3 y^2 \mathfrak{D}$$

$$(3) \qquad 3 z - \left(\frac{9 x}{2 z}\right)^2 = \frac{3 y^2 . \mathfrak{D}}{(2 z)^2}$$

Es bestehen also die beiden Kongruenzen

$$(2') \qquad 3 \xi^2 \equiv z \pmod{p^\pi},$$

wo π irgend ein positiver Exponent ist und

$$(3') \qquad \xi^2 \equiv 3 z \pmod{p^\pi}$$

Wir benutzen die Kongruenz

$$(2') \qquad 3 \xi^2 - z \equiv 0 \pmod{p^\pi}$$

Diese Kongruenz ist für jedes π lösbar.

Nach einigem Rechnen ergibt sich leicht die Identität

$$(4) \qquad 27 (\xi^3 - z \xi - x)(\xi^3 - z \xi + x) = y^2 . \mathfrak{D} + (3 \xi^2 - z)^3 - 3 z (3 \xi^2 - z)^2$$

Ist nun y teilbar durch p^π, $y^2 . \mathfrak{D}$ durch $p^{2\pi}$ (oder durch $p^{2\pi+1}$, wenn p in $\mathfrak{D}$ aufgeht), so nehmen wir $3\xi^2 - z$ teilbar durch eine genügend hohe Potenz (p^π oder $p^{\pi+1}$) dann ist

$$\xi^3 - z\xi - x$$

teilbar durch $p^{2\pi}$ oder $p^{2\pi+1}$, aber nicht durch eine höhere Potenz. Dass

$$(5) \quad \xi^3 - z\xi - x \equiv 0 \pmod{p^\pi}$$

ist, kann man annehmen, denn wäre

$$(6) \quad \xi^3 - z\xi + x \equiv 0 \pmod{p^\pi}$$

so brauchte man nur ξ in $-\xi$ zu verwandeln und erhielte aus (5)

$$(-\xi)^3 - z(-\xi) + x \equiv 0 \text{ mod } p^\pi),$$

also die Kongruenz (6).

Setzt man

$$(7) \quad \eta = -2\xi^2 + \Theta\xi + \Theta^2$$

so ist diese Zahl durch p^π teilbar,

Beweis: Die Spur von η

$$S(\eta) = \eta + \eta_1 + \eta_2 = 2(z - 3\xi^2)$$

ist teilbar durch eine beliebige Potenz von p. (p^π oder $p^{\pi+1}$).

$$A_2 = S(\eta^2) = \eta\eta_1 + \eta\eta_2 + \eta_1\eta_2 =$$
$$(3\xi^2 - z)^2 + 3\xi(\xi^3 - z\xi - x)$$

ist teilbar durch $p^{2\pi}$ oder $p^{2\pi+1}$.

Die Norm von η

$$N(\eta) = \eta\eta_1\eta_2 =$$
$$(\xi^3 - z\xi - x)^2 - 3\xi(3\xi^2 - z)(\xi^3 - z\xi - x)$$

ist teilbar durch $p^{3\pi}$ oder $p^{3\pi+2}$.

Setzt man nun

$$\eta = p^{\pi}\,\theta' = -2\,\xi^2 + \theta\,\xi + \theta^2$$

und bildet die Differenzenprodukte

$$(\eta - \eta_1)(\eta - \eta_2)(\eta_1 - \eta_2) =$$
$$p^{3\pi}(\theta' - \theta_1')(\theta' - \theta_2')(\theta_1 - \theta_2')$$

so ergibt sich

$$(8) \quad \begin{aligned} & p^{3\pi}(\theta' - \theta_1')(\theta' - \theta_2')(\theta_1 - \theta_2') = \\ & (\theta - \theta_1)(\theta - \theta_2)(\theta_1 - \theta_2)(\xi^3 - z\,\xi - x) \end{aligned}$$

Es ist

$$(\theta - \theta_1)(\theta - \theta_2)(\theta_1 - \theta_2) = y\sqrt{\mathfrak{D}}$$
$$(\theta' - \theta_1')(\theta' - \theta_2')(\theta_1' - \theta_2') = y'\sqrt{\mathfrak{D}}$$

Setzt man diese Werte in (8) ein, so erhält man

$$p^{3\pi}\,y' = (\xi^3 - z\,\xi - x)\,.\,y\,,$$

oder da $y = y_1 \,.\, p^{\pi}$ (wo y_1 nicht mehr durch p teilbar ist) so ist

$$p^{3\pi}\,y' = (\xi^3 - z\,\xi - x)\,y_1\,.\,p^{\pi}$$
$$(9) \quad p^{2\pi}\,y' = (\xi^3 - z\,\xi - x)\,y_1$$

y' ist nicht mehr durch p teilbar, wenn $\mathfrak{D}$ nicht durch p teilbar ist, oder durch p^1, wenn $\mathfrak{D}$ durch p teilbar ist.

Aus (9) folgt

$$(10) \quad y' = y_1\,.\,\frac{\xi^3 - z\,\xi - x}{p^{2\pi}}$$

$y'^2\,.\,\mathfrak{D}$ ist durch die Körperdiskriminante Δ teilbar, also

$$(11) \quad y'^2\,\mathfrak{D} = h^2\,\Delta = h^2\,.\,\lambda^2\,.\,\mathfrak{D}$$
$$(12) \quad y' = h\,.\,\lambda$$

1) Geht also p nicht in $\mathfrak{D}$ auf, so geht es auch nicht in y', also auch nicht in λ auf. Wir erhalten also als erstes Resultat: Ist x nicht durch p teilbar und geht p zu einer geraden Potenz in der Gleichungsdiskriminante auf, so ist p nicht in die Körperdiskriminante aufzunehmen.

2) Geht p in $\mathfrak{D}$ auf, so bilden wir die Gleichung für Θ_1'

(13) $\Theta_1'^3 - c\,\Theta_1'^2 + z_1'\,\Theta_1' - x_1' = 0$

Der Koeffizient

$$c = \frac{2(z - 3\xi^2)}{p^\pi}$$

ist teilbar durch p.

$$x_1' = N(\Theta') = \frac{(\xi^3 - z\xi - x)^2 - 3\xi(3\xi^2 - z)(\xi^3 - z\xi - x)}{p^{3\pi}}$$

ist teilbar durch p^2, und

$$z_1' = S(\Theta'^2) = \frac{(3\xi^2 - z)^2 + 3\xi(\xi^3 - z\xi - x)}{p^{2\pi}}$$

ist teilbar durch p, aber nicht durch p^2.

Bringt man die Gleichung (13) auf die Form

(14) $\Theta'^3 - z'\Theta' - x' = 0$,

so sieht man, da $z' = \frac{-c^2}{3} + z_1'$

$$x' = \frac{-2c^3}{27} + z_1'c - x_1',$$ dass auch die Koeffizienten

z' durch p, nicht durch p^2
x' durch p^2 teilbar sind.

Wir haben also hier den Fall, dass der Koeffizient des linearen Gliedes durch p, das absolute Glied durch p^2 teilbar ist. Diesen Fall haben wir erst in dem nächsten Abschnitt zu untersuchen.

II. x teilbar durch p.

Über die in $\varkappa$ aufgehenden Primzahlen gilt ein Satz von Dedekind [7], den wir jetzt ableiten wollen: Ist

[7] Dedekind: „Über die Diskriminanten endlicher Körper." Abhandlungen der Königlich. Gesellschaft der Wissenschaften zu Göttingen, 1882.

$\omega_1, \omega_2 \dots \omega_n$ eine Minimalbasis des Körpers, so kann man durch diese Basis alle ganzen Zahlen des Körpers darstellen, also auch $1, \theta, \theta^2 \dots \theta^{n-1}$.

$$\begin{aligned} 1 &= a_{11}\,\omega_1 + a_{12}\,\omega_2 + \dots a_{1n}\,\omega_n \\ \theta &= a_{21}\,\omega_1 + a_{22}\,\omega_2 + \dots a_{2n}\,\omega_n \\ &\vdots \\ \theta^{n-1} &= a_{n1}\,\omega_1 + a_{n2}\,\omega_2 + \dots a_{nn}\,\omega_n, \end{aligned}$$

dann ist, wie im ersten Teil gezeigt worden ist,

$$\Delta(1, \theta, \dots \theta^{n-1}) = \begin{vmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \vdots & \vdots \\ a_{n1} & a_{n2} \dots a_{nn} \end{vmatrix}^2 \Delta(\omega_1\, \omega_2 \dots \omega_n)$$

$\Delta(\omega_1\, \omega_2 \dots \omega_n)$ ist die Körperdiskriminante Δ, also

$$\begin{vmatrix} 1 & \theta & \dots \theta^{n-1} \\ 1 & \theta_1 & \dots \theta_1^{n-1} \\ \vdots & & \\ 1 & \theta_{n-1} & \dots \theta_{n-1}^{n-1} \end{vmatrix}^2 = \begin{vmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \vdots & \vdots \\ a_{n1} & a_{n2} \dots a_{nn} \end{vmatrix}^2 . \Delta$$

Die Determinante

$$\begin{vmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \vdots & \vdots \\ a_{n1} & a_{n2} \dots a_{nn} \end{vmatrix}$$

wird der „Index der Zahl θ“ genannt. Jede im Index der Zahl θ aufgehende Primzahl p heisst ein „ausserwesentlicher Teiler“ der Diskriminante im Gegensatz zu den in der Grundzahl aufgehenden „wesentlichen Teilern“. Über die im Index der Zahl θ aufgehenden Teiler gilt

der der Satz [7]): „Ist die aus lauter ganzen rationalen Zahlen a_{rs} gebildete Determinante

$$\begin{vmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \vdots & \vdots \\ a_{n1} & a_{n2} \dots a_{nn} \end{vmatrix}$$

teilbar durch p, so kann man n Zahlen $x_1, x_2 \dots x_n$, die nicht alle durch p teilbar sind, so wählen, dass die n Kongruenzen erfüllt werden

$$\left.\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots a_{1n}x_n \equiv 0 \\ a_{21}x_1 + a_{22}x_2 + \dots a_{2n}x_n \equiv 0 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots a_{nn}x_n \equiv 0 \end{array}\right\} \bmod p$$

Der Satz leuchtet von selbst ein, wenn alle a_{rs} durch p teilbar sind. Im entgegengesetzten Falle wird es eine Unterdeterminante A′ vom höchsten Grade $m < n$ geben, welche nicht durch p teilbar ist, wir dürfen annehmen, es sei dies

$$A' = \begin{vmatrix} a_{11} & a_{12} \dots a_{1m} \\ a_{21} & a_{22} \dots a_{2n} \\ \vdots & \vdots \\ a_{m1} & a_{m2} \dots a_{mm} \end{vmatrix}$$

Dann genügt man den obenstehenden Kongruenzen dadurch, dass man

$$x_{m+2} = 0, \quad x_{m+3} = 0, \dots x_n = 0$$

setzt und für $x_1, x_2 \dots x_{m+1}$ die Koeffizienten setzt, mit welchen die unbestimmten Grössen $U_1, U_2 \dots U_m, U_{m+1}$ in die Determinante

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1m}, & a_{1,m+1} \\ a_{21} & a_{22} & \dots & a_{2m} & a_{2,m+1} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mm} & a_{m,m+1} \\ U_1 & U_2 & \dots & U_m & U_{m+1} \end{vmatrix}$$

multipliziert sind, denn diese Determinante

$$U_1 x_1 + U_2 x_2 + \dots U_m x_m + U_{m+1} x_{m+1}$$

wird nach unserer Annahme, dass A' die Determinante höchsten Grades ist, die nicht durch p teilbar ist, immer eine durch p teilbare Zahl, sobald

$$U_1 = a_{r1}, U_2 = a_{r2} \dots U_m = a_{rm}, U_{m+1} = a_{r,m+1}$$

gesetzt wird. Da $x_{m+1} = A'$ nicht durch p teilbar ist, so ist der Satz bewiesen.

Geht also p im Index von Θ, in $\varkappa$, auf, so kann man in unserem Falle, wo $n = 3$ ist die Kongruenzen lösen:

$$a_{r1} x_1 + a_{r2} x_2 + a_{r3} x_3 \equiv 0 \pmod{p},$$

und da 1, θ, θ^2 ganze Zahlen sind, auch die Kongruenz

$$\alpha + \beta \theta + \gamma \theta^2 \equiv 0 \pmod{p}.$$

Es gibt also in diesem Falle eine Zahl

$$\eta = \frac{\alpha + \beta \theta + \gamma \theta^2}{p},$$

welche ganz ist, ohne dass die Koeffizienten α, β, γ alle drei durch p teilbar sind. Kann man also eine solche Zahl η finden, so geht p mindestens zur ersten Potenz in $\varkappa$ auf. Es gilt auch das Umgekehrte: Wenn p in $\varkappa$ aufgeht, so kann man die Koeffizienten α, β, γ, die nicht alle durch p teilbar sind, so bestimmen, dass die Zahl

$$\eta = \frac{\alpha + \beta \theta + \gamma \theta^2}{p}$$

ganz wird. Der Satz hat auch Gültigkeit für $p = 2$ und $p = 3$.

1) Es sei x nun durch p, nicht durch p^2 teilbar. In diesem Falle ist Θ^2 nicht $\equiv 0 \pmod{p}$ weil $N\left(\frac{\Theta^2}{p}\right) = \frac{x^2}{p^3}$ keine ganze Zahl ist.

Dann ist auch, wie man aus

$$y^2 \mathfrak{D} = 4 z^3 - 27 x^2$$

ersieht, z durch p teilbar. y ist durch p, nicht durch p^2 teilbar. $\mathfrak{D}$ ist durch p nicht teilbar. Ist nun

$$\eta_1 = \alpha + \beta \Theta + \gamma \Theta^2$$

durch p teilbar, so folgt zunächst aus

$$S(\eta_1) = 3\alpha + 2\gamma z,$$

dass α durch p teilbar sein muss; also muss

$$\beta \Theta + \gamma \Theta^2$$

durch p teilbar sein, also auch

$$\beta \Theta^2 + \gamma \Theta^3.$$

Da nun

$$\Theta^3 = z\Theta + x$$

durch p teilbar ist, muss $\beta \Theta^2$ durch p teilbar sein, und da Θ^2 nicht $\equiv 0 \pmod{p}$, muss β durch p teilbar sein und folglich auch γ. Die Zahl

$$\eta = \frac{\alpha + \beta \Theta + \gamma \Theta^2}{p}$$

ist nicht ganz (ausser wenn α, β, γ durch p teilbar sind). Folglich ist $\varkappa$ nicht durch p teilbar, also ist λ durch p, nicht durch p^2 teilbar.

R e s u l t a t: Ist x teilbar durch p, nicht durch p^2, so geht p in λ einfach auf.

2) Es sei x durch p^2 teilbar, z mindestens durch p. In diesem Falle ist die Zahl

$$(15) \quad \Theta' = \frac{3\,\Theta^2 - 2\,z}{p}$$

ganz, denn es ist, wenn

$$(16) \quad \Theta'^3 - z'\,\Theta' - x' = 0 \quad \text{ist,}$$

$$(17) \quad z' = \frac{3\,z^2}{p^2} \quad \text{ganz}$$

$$(18) \quad x' = \frac{27\,x^2}{p^3} - \frac{2\,z^3}{p^3} \quad \text{ganz.}$$

Wir unterscheiden

a) z nicht durch p^2 teilbar,

b) z durch p^2 teilbar.

a) Ist z nicht durch p^2 teilbar, so ist z′ nicht durch p teilbar, und x′ ist auch nicht durch p teilbar. Die Diskriminante der Gleichung (16) ist

$$y'^2 \,.\, \mathfrak{D} = 4\,z'^3 - 27\,x'^2 =$$

$$4\left(\frac{3\,z^2}{p^2}\right)^3 - 27\left(\frac{27\,x^2}{p^3} - \frac{2\,z^3}{p^3}\right)^2$$

oder

$$(19) \quad y'^2\,\mathfrak{D} = \frac{4\,.\,27^2\,x^2\,z^2}{p^6} - \frac{27^3\,x^4}{p^6}$$

Da die rechte Seite von (19) nur noch durch p^1 teilbar ist, kann y'^2 nicht durch p teilbar sein. Also geht p auch nicht in λ auf.

Resultat: Ist x durch p^2, z durch p, nicht durch p^2 teilbar, so ist p nicht in λ aufzunehmen.

Damit ist auch der Fall I. 2. erledigt, den wir auf den soeben behandelten Fall zurückgeführt hatten.

b) Ist z durch p^2, x durch p^2, nicht durch p^3 teilbar, so ist

z' durch p^2,
x' durch p, nicht durch p^2 teilbar.

Der Koeffizient des linearen Gliedes ist durch p^2, das absolute Glied durch p teilbar. Diesen Fall haben wir schon in II. 1. behandelt, und es ergibt sich also hier auch, dass p einfach in λ aufgeht.

Resultat: Ist x durch p^2, z durch p^2 teibar, so ist p einfach in λ aufzunehmen.

Wir erhalten als

Gesamtresultat für die Primzahl $p > 3$.

Eine von 2 und 3 verschiedene Primzahl p, die in y aufgeht, ist nur dann in λ und zwar einfach, aufzunehmen :

1) wenn p in x einfach aufgeht,

2) wenn p in x zweifach und in z zweifach aufgeht.

Wir betrachten jetzt die Spezialfälle, die Primzahlen 2 und 3.

4. Die Primzahl 2.

Wir nehmen an, dass nicht zugleich x durch 8 und z durch 4 teilbar sei, denn wäre dies der Fall, so würde man setzen

$$x = 8 . x_1 \quad z = 4 z_1 , \quad \theta = 2 \theta_1$$

und würde erhalten die Gleichung

$$\theta_1^3 - z_1 \theta_1 - x_1 = 0 ,$$

die man dann statt der ursprünglichen

$$\theta^3 - z \theta - x = 0$$

zu untersuchen hätte.

Aus

$$y^2 \mathfrak{D} = 4\,z^3 - 27\,x^2$$

ersieht man, dass 2 nur dann in y aufgeht, wenn es in x aufgeht.

Wir unterscheiden folgende zwei Hauptfälle:

I. z ist gerade

II. z ist ungerade.

Im Falle I. haben wir folgende Spezialfälle zu unterscheiden:

α) x durch 2 teilbar, nicht durch 4,
z durch 2^{σ} teilbar.

β) x durch 4 teilbar, nicht durch 8,
z durch 2^{σ} teilbar.

γ) x durch 8 teilbar,
z durch 2 teilbar, nicht durch 4.

Wir untersuchen den ersten Fall:

α) x durch 2 teilbar, nicht durch 4,
z durch 2^{σ} teilbar.

Aus

$$y^2 . \mathfrak{D} = 4\,z^3 - 27\,x^2$$

ergibt sich, dass y nur durch 2 teilbar sein kann. Die Zahl

$$\eta = \frac{\alpha + \beta\,\Theta + \gamma\,\Theta^2}{2}$$

kann nur ganz sein, wenn

$$\alpha \equiv 0, \quad \beta \equiv 0, \quad \gamma \equiv 0 \pmod 2$$

ist, denn aus

$$2\,S(\eta) = 3\,\alpha + 2\,\gamma\,z \equiv 0 \pmod 2$$

folgt

$$\alpha \equiv 0 \pmod 2).$$

Da

$$\Theta^3 = z\,\Theta + x \equiv 0 \pmod 2$$

ist, und Θ^2 nicht $= 0 \pmod 2$, weil $N\left(\frac{\Theta^2}{2}\right) = \frac{x^2}{8}$ keine ganze Zahl ist, muss in der Zahl

$$\Theta \,.\, \eta = \frac{\Theta\alpha + \beta\,\Theta^2 + \gamma\,\Theta^3}{2}$$

$$\beta \equiv 0 \pmod 2$$

sein und folglich auch

$$\gamma \equiv 0 \pmod 2$$

2 kann also nicht im Index der Zahl Θ, in $\varkappa$, aufgehen, es muss λ enthalten sein.

R e s u l t a t: Ist x durch 2 teilbar, nicht durch 4, z durch 2^σ, so geht 2 einfach in λ auf.

β) x durch 4 teilbar, nicht durch 8, z durch 2^σ,

$$x = 4\,x_1 \qquad z = 2^\sigma\,z_1\,.$$

Wie man aus

$$y^2\,\mathfrak{D} = 4\,z^3 - 27\,x^2 = 4\,.\,2^{3\sigma}\,z_1{}^3 - 27\,.\,4^2\,.\,x_1{}^2$$

sieht, ist in diesem Falle y durch 4 teilbar, nicht durch 8.

Die Zahl

$$\eta = \frac{\Theta^2}{2}$$

ist ganz, denn

$$S(\eta) = \frac{2\,z}{2} \text{ ist ganz,}$$

$$S(\eta^2) = \frac{z^2}{4} \text{ ist ganz,}$$

$$N(\eta) = \frac{x^2}{8} \text{ ist ganz.}$$

Die Primzahl 2 geht also mindestens zur ersten Potenz in $\varkappa$ auf. Da aber y durch 4 teilbar ist, ist zu untersuchen, ob $\varkappa$ durch 4 teilbar ist oder nur durch 2. Ist

$$\eta = \frac{\alpha + \beta\,\theta + \gamma\,\theta^2}{2},$$

so ist $\qquad 1 \quad \theta \quad \eta$

eine Basis des Körpers, also wenn

$$\begin{aligned} 1 &= a_{11}\,\omega_1 + a_{12}\,\omega_2 + a_{13}\,\omega_3 \\ \theta &= a_{21}\,\omega_1 + a_{22}\,\omega_2 + a_{23}\,\omega_3 \\ \eta &= a_{31}\,\omega_1 + a_{32}\,\omega_2 + a_{33}\,\omega_3 \end{aligned}$$

so ist die Diskriminante dieser Basis

$$\Delta(1, \theta, \eta) = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}^2 . \Delta(\omega_1\, \omega_2\, \omega_3)$$

$$= \varkappa_1^2 . \Delta$$

oder

$$\begin{vmatrix} 1 & \theta & \eta \\ 1 & \theta' & \eta' \\ 1 & \theta'' & \eta'' \end{vmatrix}^2 = \begin{vmatrix} 1, \theta, \dfrac{\alpha + \beta\,\theta + \gamma\,\theta^2}{2} \\ 1, \theta', \dfrac{\alpha + \beta\,\theta' + \gamma\,\theta'^2}{2} \\ 1, \theta'', \dfrac{\alpha + \beta\,\theta'' + \gamma\,\theta''^2}{2} \end{vmatrix}^2$$

$$= \frac{\gamma^2}{4} \begin{vmatrix} 1 & \theta & \theta^2 \\ 1 & \theta' & \theta'^2 \\ 1 & \theta'' & \theta''^2 \end{vmatrix}^2 = \frac{\gamma^2}{4} \varkappa^2 . \Delta = \varkappa_1^2\, \Delta$$

Hieraus folgt

$$\varkappa_1 = \frac{\gamma}{2}\,\varkappa$$

$$\lambda\varkappa_1 = \frac{\gamma}{2}\,y$$

$\varkappa_1$ ist nicht durch 2 teilbar, also ist λ durch 2 teilbar.

Resultat: Ist x durch 4 teilbar, nicht durch 8, z durch 2^3, so geht 2 einfach in λ auf.

γ) x durch 8 teilbar, z durch 2, nicht durch 4.

$$x = 8 x_1 \qquad z = 2 z_1$$

Aus

$$y^2 . \mathfrak{D} = 4 . z^3 - 27 x^2 = 4 . 8 . z_1^3 - 27 . 8^2 x_1^2$$

folgt, dass y durch 4 teilbar ist. Wir haben hier genau denselben Fall wie β und erhalten daher das

Resultat: Ist x durch 8 teilbar, z durch 2, nicht durch 4, so geht 2 einfach in λ auf.

Gesamtresultat für den Fall I: Sind x und z gerade, so ist 2 einfach in λ aufzunehmen.

II. x gerade, z ungerade.

Hierbei machen wir folgende Unterscheidungen:

α) $x \equiv 0 \pmod 4$, $z \equiv 1 \pmod 4$
β) $x \equiv 0 \pmod 4$, $z \equiv 3 \pmod 4$
γ) $x \equiv 2 \pmod 4$, $z \equiv 1 \pmod 4$
δ) $x \equiv 2 \pmod 4$, $z \equiv 3 \pmod 4$

In den Fällen α) und δ) ist die Zahl

$$\eta = \frac{\Theta + \Theta^2}{2}$$

ganz, denn

$$S(\eta) = \frac{2z}{2} \quad \text{ist ganz}$$

$$S(\eta^2) = \frac{z^3 - 3x - z}{4} \quad \text{ist ganz}$$

$$N(\eta) = \frac{x^2 - xz + x}{8} = \frac{x^2}{8} - \frac{x(z-1)}{8}$$

ist ganz.

Wir untersuchen

$$\alpha)\quad x \equiv 0 \pmod 4 \quad z \equiv 1 \pmod 4$$

$$z = 4 z_1 + 1$$

$$y^2 . \mathfrak{D} = 4 [64 z_1^3 + 48 z_1^2 + 12 z_1 + 1] - 27 x^2$$

y ist durch 2 teilbar.

$$\mathfrak{D} \equiv 1 \pmod 4$$

2 geht in $\varkappa$ auf.

Resultat: Ist $\left.\begin{array}{l} x \equiv 0 \\ z \equiv 1 \end{array}\right\} \pmod 4$,

so geht 2 nicht in λ auf.

$$\beta)\qquad \left.\begin{array}{l} x \equiv 0 \\ z \equiv 3 \end{array}\right\} \pmod 4$$

$$y^2 . \mathfrak{D} = 4 z^3 - 27 x^2 =$$

$$4 [64 z_1^3 + 3 . 16 . 3 z_1^2 + 3 . 4 . 9 z_1 + 27] - 27 x^2$$

$$(z = 4 z_1 + 3)$$

y ist durch 2 teilbar. Die Zahl

$$\eta = \frac{\alpha + \beta \Theta + \gamma \Theta^2}{2}$$

ist nur ganz, wenn $\alpha \equiv 0 \pmod 2$, $\beta \equiv 0 \pmod 2$, $\gamma \equiv 0 \pmod 2$, denn aus

$$2 S(\eta) = 3 \alpha + 2 \gamma z \equiv 0 \pmod 2$$

folgt

$$\alpha \equiv 0 \pmod 2.$$

Aus

$$4 S(\eta^2) = \begin{vmatrix} 3 \alpha + \gamma z\,, & \beta \\ 3 \gamma x + \beta z, & \alpha + \gamma z \end{vmatrix} \equiv 0 \pmod 4$$

ergibt sich, da $x \equiv 0$, $z \equiv 3$, $\alpha \equiv 2 \pmod 4$

$$\begin{vmatrix} 6 + 3 \gamma, & \beta \\ 3 z\,, & 2 + 3 \gamma \end{vmatrix} \equiv 0 \pmod 4$$

oder

$$\begin{vmatrix} 2+\gamma & \beta \\ z & 2+3\gamma \end{vmatrix} \equiv 0 \pmod 4$$

oder

$$4 + 8\gamma - \beta^2 \equiv 0 \pmod 4$$
$$\beta \equiv 0 \pmod 2$$

Da Θ^2 nicht $\equiv 0 \pmod 2$ ist, so ist auch

$$\gamma \equiv 0 \pmod 2$$

2 geht daher in diesem Falle nicht in K auf.

Resultat: Ist $\left.\begin{matrix} x \equiv 0 \\ z \equiv 3 \end{matrix}\right\} \pmod 4$

so ist 2 einfach in λ aufzunehmen.

γ) $\left.\begin{matrix} x \equiv 2 \\ z \equiv 1 \end{matrix}\right\} \pmod 4$

$$x = 2x_1 + 2$$
$$z = 4z_1 + 1$$
$$y^2 . \mathfrak{D} = 4z^3 - 27x^2 =$$
$$4[64z_1^3 + 48z_1^2 + 12z_1 + 1] - 27[16x_1^2 + 16x_1 + 4]$$

y ist durch 2 teilbar.

$$\mathfrak{D} \equiv 2 \pmod 4$$

Die Zahl

$$\eta = \frac{\alpha + \beta\Theta + \gamma\Theta^2}{2}$$

ist nur ganz, wenn $\alpha \equiv 0 \pmod 2$, $\beta \equiv 0 \pmod 2$, $\gamma \equiv 0 \pmod 2$ ist.

Aus

$$2\,S(\eta) = 3\alpha + 2\gamma z \equiv 0 \pmod 2$$

folgt

$$\alpha \equiv 0 \pmod 2.$$

Aus

$$8\,N(\eta) = \begin{vmatrix} \alpha & \beta & \gamma \\ \gamma x & a + \gamma z & \beta \\ \beta x & \gamma x + \beta z & \alpha + \gamma z \end{vmatrix} \equiv 0 \pmod 8$$

ergibt sich, da

$$\alpha \equiv 2 \pmod 4$$
$$x \equiv 2 \pmod 4$$
$$z \equiv 1 \pmod 4$$

$$\begin{vmatrix} 2 & \beta & \gamma \\ 2\gamma & 2 + 2\gamma & \beta \\ 2\beta & 2\gamma + 2\beta & 2 + 2\gamma \end{vmatrix} \equiv 0 \pmod 4$$

oder

$$\begin{vmatrix} 1 & \beta & \gamma \\ \gamma & 2 + 2\gamma & \beta \\ \beta & 2\gamma + 2\beta & 2 + 2\gamma \end{vmatrix} \equiv 0 \pmod 2$$

oder

$$(2 + 2\gamma)(2 + 2\gamma) - 2\gamma\beta - 2\beta^3 + \beta^3 - 2\gamma\beta - 2\beta\gamma^2$$
$$+ 2\gamma^3 + 2\gamma^2\beta - 2\gamma\beta - 2\gamma^2\beta \equiv 0 \pmod 2.$$

Daraus folgt

$$\beta^3 \equiv 0 \pmod 2$$
$$\beta \equiv 0 \pmod 2$$

und da Θ^2 nicht $\equiv 0 \pmod 2$, auch

$$\gamma \equiv 0 \pmod 2$$

2 geht also in λ auf.

Resultat: Ist $\left.\begin{matrix} x \equiv 2 \\ z \equiv 1 \end{matrix}\right\} \bmod 4$,

so geht 2 einfach in λ auf.

δ) Es bleibt der Fall:

$$\left.\begin{matrix} x \equiv 2 \\ z \equiv 3 \end{matrix}\right\} \bmod 4$$

$$x = 4x_1 + 2; \quad z = 4z_1 + 3$$

$$y^2 . \mathfrak{D} = 4z^3 - 27x^2 =$$

$$4[4 . 4 . 4z_1^3 + 3 . 3 . 4 . 4z_1^2 + 3 . 3 . 3 . 4z_1 + 27]$$

$$- 27[4 . 4x_1^2 + 4 . 4x_1 + 4] =$$

$$2^8 z_1^3 + 3^2 . 2^6 z_1^2 + 3^2 . 2^4 z_1 - 3^3 . 2^4 x_1^2 - 3^2 . 2^4 x_1$$

In diesem Falle ist y mindestens durch 2^2 teilbar. Es kann aber auch noch durch eine höhere Potenz von 2 teilbar sein, wenn nämlich x_1 und z_1 noch durch 2 teilbar sind. In diesem Falle kann man die Kongruenz

$$3\xi^2 - z \equiv 0 \pmod{2^\sigma}$$

für ein beliebiges σ lösen. Setzt man nun wieder

$$\eta = -2\xi^2 + \xi\theta + \theta^2,$$

$$\eta^3 - a_1\eta^2 + a_2\eta - a_3 = 0,$$

wo

$$a_1 = 2(z - 3\xi^2)$$

$$a_2 = (3\xi^2 - z)^2 + 3\xi(\xi^3 - z\xi - x)$$

$$a_3 = (\xi^3 - z\xi - x)^2 + 3\xi(3\xi^2 - z)(\xi^3 - z\xi - x),$$

und wo die Identität besteht

$$27(\xi^3 - z\xi - x)(\xi^3 - z\xi + x) =$$

$$y^2 . \mathfrak{D} + (3\xi^2 - z)^3 - 3z(3\xi^2 - z)^2,$$

aus der sich ergibt, dass

$$\xi^3 - z\xi - x \equiv 0 \pmod{2^\sigma}$$

ist, so ist

$$\frac{\eta}{2^\sigma} = \frac{-2\xi^2 + \xi\theta + \theta^2}{2^\sigma}$$

eine ganze Zahl, und wie in dem allgemeinem Falle p erhält man durch dieselben Schlüsse wie dort das

Resultat: Ist $\left.\begin{array}{l} x \equiv 2 \\ z \equiv 3 \end{array}\right\} \bmod 4$

so ist 2 nicht in λ aufzunehmen. Ist also z ungerade, so geht 2 nur in folgenden 2 Fällen in λ auf:

1) wenn $\left.\begin{matrix} x \equiv 0 \\ z \equiv 3 \end{matrix}\right\}$ mod 4

2) wenn $\left.\begin{matrix} x \equiv 2 \\ z \equiv 1 \end{matrix}\right\}$ mod 4.

Gesamtresultat für die Primzahl 2:

Die Primzahl 2 geht in folgenden Fällen in λ auf und zwar einfach:

1) wenn x und z gerade sind,

2) wenn z ungerade ist, in den beiden Fällen:

a) $\left.\begin{matrix} x \equiv 0 \\ z \equiv 3 \end{matrix}\right\}$ mod 4. $\mathfrak{D} \equiv 3 \pmod 4$

b) $\left.\begin{matrix} x \equiv 2 \\ z \equiv 1 \end{matrix}\right\}$ mod 4. $\mathfrak{D} \equiv 2 \pmod 4$

5. Die Primzahl 3.

Wir nehmen an, dass in

$$\theta^3 - z\theta - x = 0$$

nicht zugleich x durch 27 und z durch 9 teilbar sei; denn wäre dies der Fall, so würde man setzen

$$x = 27\, x_1$$
$$z = 9\, z_1$$
$$\theta = 3\, \theta_1$$

und erhielte die Gleichung

$$\theta_1^3 - z_1 \theta_1 - x_1 = 0\,,$$

die man dann statt der ursprünglichen zu untersuchen hätte. Aus

$$y^2 . \mathfrak{D} = 4\, z^3 - 27\, x^2$$

sieht man, dass 3 nur dann in y aufgeht, wenn es in z aufgeht.

Wir unterscheiden die beiden Hauptfälle:

I. $x \equiv 0 \pmod 3$

II. x nicht $\equiv 0 \pmod 3$

I. α) x sei durch 3 teilbar, nicht durch 9, z sei durch 3 teilbar, nicht durch 9.

$$x = 3\,x_1 \qquad z = 3\,z_1$$

$$y^2 \,.\, \mathfrak{D} = 4\,z^3 - 27\,x^2 = 4\,.\,3\,.\,3\,.\,3\,z_1^3 - 27\,.\,9\,.\,x_1^2$$

y ist durch 3 teilbar und
$\mathfrak{D}$ ist durch 3 teilbar.

Die Zahl

$$\eta = \frac{\alpha\,\Theta + \beta + \gamma\,\Theta^2}{3}$$

ist nur ganz, wenn

$$\alpha \equiv 0, \quad \beta \equiv 0, \quad \gamma \equiv 0 \pmod 3),$$

denn ist

$$\eta = \frac{\alpha + \beta\,\Theta + \gamma\,\Theta^2}{3}$$

ganz, so muss

$$N(\eta) = \frac{1}{27}\begin{vmatrix} \alpha & \beta & \gamma \\ \gamma x & \alpha + \gamma z & \beta \\ \beta x & \gamma x + \beta z, & \alpha + \gamma z \end{vmatrix}$$

rational und ganz sein, d. h.

$$\begin{vmatrix} \alpha & \beta & \gamma \\ \gamma x & \alpha + \gamma z & \beta \\ \beta x & \gamma x + \beta z & \alpha + \gamma z \end{vmatrix} \equiv 0 \pmod 3)$$

oder, da $\left.\begin{matrix} x \equiv 0 \\ z \equiv 0 \end{matrix}\right\}$ mod 3,

$$\begin{vmatrix} \alpha & \beta & \gamma \\ 0 & \alpha & \beta \\ 0 & 0 & \alpha \end{vmatrix} \equiv 0 \pmod 3)$$

$$\alpha^3 \equiv 0 \pmod 3)$$

$$\alpha \equiv 0 \pmod 3).$$

Da

$$\theta^3 = z\,\theta + x \equiv 0 \pmod 3$$

und

$$\theta^2 \text{ nicht} \equiv 0 \pmod 3,$$

so muss in

$$\alpha\,\theta + \beta\,\theta^2 + \gamma\,\theta^3$$
$$\beta \equiv 0 \pmod 3$$

sein, also auch

$$\gamma \equiv 0 \pmod 3$$

3 kann also nicht in $\varkappa$ aufgehen.

Resultat: Ist x durch 3 teilbar, z durch 3, so ist 3 einfach in λ aufzunehmen.

β) z sei durch 9 teilbar
x durch 3.

$$z = 9 \,.\, z_1 \qquad x = 3\,x_1$$
$$y^2 \,.\, \mathfrak{D} = 4\,z^3 - 27\,x^2 =$$
$$4 \,.\, 9 \,.\, 9 \,.\, 9\,z_1^3 - 27 \,.\, 9 \,.\, 9 \,.\, x_1^2$$

y ist durch 27 teilbar
$\mathfrak{D}$ ist nicht durch 3 teilbar.

Die Zahl

$$\eta = \frac{\alpha + \beta\,\theta + \gamma\,\theta^2}{3}$$

ist nur ganz, wenn

$$\alpha \equiv 0, \quad \beta \equiv 0, \quad \gamma \equiv 0 \pmod 3$$

ist, denn wie eben, ergibt sich aus $N(\eta)$, dass $\alpha \equiv 0 \pmod 3$ ist, und folglich auch $\beta \equiv 0$, $\gamma \equiv 0 \pmod 3$

3 geht also nicht in $\varkappa$ auf.

Resultat: Ist z durch 9 teilbar, x durch 3, so ist λ durch 3^2 teilbar.

γ) z sei durch 3 teilbar,
x durch 9

$$z = 3\,z_1, \qquad x = 9\,x_1$$
$$y^2 \,.\, \mathfrak{D} = 4 \,.\, z^3 - 27\,x^2 = 4 \,.\, 27\,z_1^3 - 27 \,.\, 9^2\,x_1^2$$

y ist durch 3 teilbar
$\mathfrak{D}$ ist durch 3 teilbar.

Die Zahl

$$\eta = \frac{\Theta^2}{3}$$

ist ganz, denn

$$S(\eta) = \frac{2z}{3}$$

ist rational und ganz,

$$S(\eta^2) = \frac{z^2 - 3x}{9}$$

ist rational und ganz

$$N(\eta) = \frac{x^2}{27}$$

ist rational und ganz.

Also geht 3 in $\varkappa$ auf.

Resultat: Ist z durch 3 teilbar, x durch 9, so geht 3 nicht in λ auf.

δ) x sei durch 9 teilbar und
z sei durch 9 teilbar

$$y^2 . \mathfrak{D} = 4z^3 - 27x^2 = 4 . 9 . 9 . 9 z_1^3 - 27 . 9 . 9 x_1^2$$

y ist durch 27 teilbar.

Die Zahl

$$\eta = \frac{\Theta^2}{3}$$

ist ganz.

Wir bilden die Diskriminante der Basis $(1, \Theta, \eta)$

$$\Delta(1, \Theta, \eta) = \begin{vmatrix} 1 & \Theta & \frac{\Theta^2}{3} \\ 1 & \Theta' & \frac{\Theta'^2}{3} \\ 1 & \Theta'' & \frac{\Theta''^2}{3} \end{vmatrix}^2$$

$$= \varkappa_1^2 . \Delta = \frac{1}{9} \varkappa^2 . \lambda^2 . \mathfrak{D}$$

$$\lambda \cdot \varkappa_1 = \frac{1}{3} y$$

$\varkappa_1$ ist nicht durch 3 teilbar. Also ist λ durch 3^2 teilbar.

Resultat: Ist x durch 9 teilbar, z durch 9, so geht 3^2 in λ auf.

ε) x sei durch 27, z durch 3 teilbar.

$$x = 27\, z_1 \qquad z = 3\, z_1$$

$$y^2 \cdot \mathfrak{D} = 4\, z^3 - 27\, x^2 = 4 \cdot 3 \cdot 3 \cdot 3\, z_1^3 - 27 \cdot 27 \cdot 27\, x_1^2$$

y ist durch 3 teilbar.

$$\eta = \frac{\Theta^2}{3}$$

ist eine ganze Zahl. Also geht 3 in $\varkappa$ auf.

Resultat: Ist x durch 27, z durch 3 teilbar, so ist 3 nicht in λ aufzunehmen.

Gesamtresultat für I.

Ist $x \equiv 0 \pmod 3$, so ist

1) 3 einfach in λ aufzunehmen, wenn x durch 3 teilbar ist, und z durch 3;
2) 3 zweifach in λ aufzunehmen, wenn z durch 9, x durch 3 oder durch 9 teilbar ist.

Wir kommen zu dem Fall II:

$$x \text{ nicht} \equiv 0 \pmod 3$$

Wir unterscheiden:

a) $z \equiv 0 \pmod 9$

$$\left.\begin{array}{ll} 1) & x \equiv \pm 1 \\ 2) & x \equiv \pm 2 \\ 3) & x \equiv \pm 4 \end{array}\right\} \bmod 9$$

b) $z \equiv 3 \pmod 9$

$$\left.\begin{array}{ll} 1) & x \equiv \pm 1 \\ 2) & x \equiv \pm 2 \\ 3) & x \equiv \pm 4 \end{array}\right\} \bmod 9$$

c) $z \equiv 6 \pmod 9$

$$\left.\begin{array}{l} 1)\ x \equiv \pm 1 \\ 2)\ x \equiv \pm 2 \\ 3)\ x \equiv \pm 4 \end{array}\right\} \bmod 9$$

a) 1. $$\left.\begin{array}{l} z \equiv 0 \\ x \equiv \pm 1 \end{array}\right\} \bmod 9$$

$$z = 9\, z_1 \qquad x = 9\, x_1 \pm 1$$

$$y^2 . \mathfrak{D} = 4\, z^3 - 27\, x^2 =$$

$$4 . 9^3\, z_1^3 - 27 . 9^2\, x_1^2 \mp 2 . 27 . 9\, x_1 - 27$$

y ist durch 3 teilbar.

$\mathfrak{D}$ ist durch 3 teilbar.

Die Zahl

$$\eta = \frac{\theta^2 \pm \theta + 1}{3}$$

ist ganz, denn

$$S(\eta) = \frac{3 + 2\, z}{3}$$

ist rational und ganz,

$$S(\eta^2) = \frac{z^2 + 3\, z - 3\, (\pm x - 1)}{9}$$

ist rational und ganz, und

$$N(\eta) = \frac{(\pm x + 1)\, (\pm x + 1 + z) + z^2}{27}$$

ist rational und ganz.

3 geht also in $\varkappa$ auf.

Resultat: Ist z durch 9 teilbar, $x \equiv \pm 1 \pmod 9$, so ist λ nicht durch 3 teilbar.

a) 2. $$\left.\begin{array}{l} z \equiv 0 \\ x \equiv \pm 2 \end{array}\right\} \bmod 9$$

$$z = 9\, z_1 \qquad x = 9\, x_1 \pm 2$$

$$y^2 . \mathfrak{D} = 4\, z^3 - 27\, x^2$$

$$= 4 . 9^3\, z_1^3 - 27 . 9^2\, x_1^2 \mp 27 . 2 . 9\, x_1 - 27 . 4$$

y ist durch 3 teilbar.

$\mathfrak{D}$ ist durch 3 teilbar.

Die Zahl

$$\eta = \frac{\alpha + \beta\Theta + \gamma\Theta^2}{3}$$

ist nur ganz, wenn

$$\alpha \equiv 0, \quad \beta \equiv 0, \quad \gamma \equiv 0 \pmod{3}$$

ist. Also geht 3 in λ auf.

Resultat: Ist $\left.\begin{array}{l} z \equiv 0 \\ x \equiv \pm 2 \end{array}\right\} \bmod 9$,

so geht 3 einfach in λ auf.

a) 3. $\left.\begin{array}{l} z \equiv 0 \\ x \equiv \pm 4 \end{array}\right\} \bmod 9$

$$z = 9\,z_1 \qquad x = 9\,x_1 \pm 4$$

$$y^2 . \mathfrak{D} = 4\,z^3 - 27\,x^2$$

$$= 4 . 9^3 z_1^3 - 27 . 9^2 x_1^2 \mp 8 . 9 . 27\,x_1 - 27 . 16$$

y ist durch 3 teilbar.

$\mathfrak{D}$ ist durch 3 teilbar.

Da die Zahl

$$\eta = \frac{\alpha + \beta\Theta + \gamma\Theta^2}{3}$$

nur ganz ist, wenn $\alpha \equiv 0$, $\beta \equiv 0$, $\gamma \equiv 0 \pmod{3}$ ist, so kann 3 nicht in $\varkappa$ aufgehen.

Resultat: Ist $\left.\begin{array}{l} z \equiv 0 \\ x \equiv \pm 4 \end{array}\right\} \bmod 9$

so geht 3 einfach in λ auf.

Gesamtresultat für a:

Ist $\left.\begin{array}{ll} x \text{ nicht} \equiv 0 & \bmod 3 \\ z \equiv 0 & \bmod 9, \end{array}\right.$

so geht 3 in λ auf, wenn

$\left.\begin{array}{l} x \equiv \pm 2 \\ x \equiv \pm 4 \end{array}\right\} \bmod 9$

oder ist.

b) $z \equiv 3 \pmod{9}$.

In allen diesen Fällen ist y mindestens durch 3^2 teilbar. Es kann aber auch noch durch eine höhere Potenz von 3 teilbar sein. Wir untersuchen zuerst den Fall, dass y nur durch 3^2 teilbar ist.

Nur wenn

$$x \equiv \pm 2 \pmod 9,$$

ist die Zahl

$$\eta = \frac{\alpha + \beta\Theta + \gamma\Theta^2}{3}$$

ganz, ohne dass die Koeffizienten einzeln durch 3 teilbar sind. Diese Zahl ist

$$\eta = \frac{1 \mp \Theta + \Theta^2}{3},$$

denn

$$S(\eta) = \frac{3 + 2z}{3}$$

ist rational und ganz,

$$S(\eta^2) = \frac{z^2 + 3z \pm 3(x \pm 1)}{9}$$

ist rational und ganz,

$$N(\eta) = \frac{(\pm x + 1 + z)(\pm x + 1) + z^2}{27}$$

ist rational und ganz.

Bildet man wieder die Diskriminante der Basis $(1, \Theta, \eta)$

$$\Delta(1, \Theta, \eta) = \begin{vmatrix} 1 & \Theta, & \frac{1 - \Theta + \Theta^2}{3} \\ 1 & \Theta', & \frac{1 - \Theta' + \Theta'^2}{3} \\ 1 & \Theta'', & \frac{1 - \Theta'' + \Theta''^2}{3} \end{vmatrix}^2$$

$$= \frac{1}{9} \begin{vmatrix} 1 & \Theta & \Theta^2 \\ 1 & \Theta' & \Theta'^2 \\ 1 & \Theta'' & \Theta''^2 \end{vmatrix}^2 = \varkappa_1^2 \Delta,$$

so ist
$$\lambda \varkappa_1 = \frac{1}{3} y,$$
und da $\varkappa_1$ nicht durch 3 teilbar ist, $\lambda \equiv 0 \pmod 3$.

Resultat: Ist y durch 9 teilbar,
$$\left.\begin{matrix} z \equiv 3 \\ x \equiv \pm 2 \end{matrix}\right\} \bmod 9$$
so ist 3 einfach in λ aufzunehmen.

In den Fällen

b) 2. $$\left.\begin{matrix} z \equiv 3 \\ x \equiv \pm 1 \end{matrix}\right\} \bmod 9$$

und b) 3. $$\left.\begin{matrix} z \equiv 3 \\ x \equiv \pm 4 \end{matrix}\right\} \bmod 9$$

ergibt sich durch Ausrechnen der symmetrischen Grundfunktionen von $S(\eta)$, $S(\eta^2)$ und $N(\eta)$, dass die Zahl
$$\eta = \frac{\alpha + \beta\,\Theta + \gamma\,\Theta^2}{3}$$
nur ganz ist, wenn $\alpha \equiv 0 \pmod 3$, $\beta \equiv 0 \pmod 3$, $\gamma \equiv 0 \pmod 3$ ist.

In diesen beiden Fällen ist also λ durch 3^2 teilbar.

Resultat; Ist y durch 9 teilbar,
$$z \equiv 3 \pmod 9$$
$$\left.\begin{matrix} x \equiv \pm 1 \\ \text{oder} \quad x \equiv \pm 4 \end{matrix}\right\} \bmod 9,$$
so ist λ durch 3^2 teilbar.

Wir untersuchen jetzt den Fall, dass y durch eine höhere Potenz als die zweite von 2 teilbar ist. Ist z. B.
$$z \equiv 3 \pmod 9$$
$$x \equiv \pm 1 \pmod 9,$$
so setzen wir
$$z = 9\,z_1 + 3; \qquad x = 9\,x_1 \pm 1$$
$$y^2\,\mathfrak{D} = 4\,z^3 - 27\,x^2 =$$
$$4 \cdot 9^3 z_1^3 + 4 \cdot 9^3 z_1^2 + 4 \cdot 9^2 z_1 - 27 \cdot 9^2 x_1^2 \mp 18 \cdot 27\,x_1$$

Sind z_1 und x_1 noch durch 3 teilbar, so ist y durch 3^σ teilbar, wo $\sigma > 2$. In diesem Falle ist die Kongruenz

$$3\,\xi^2 - z \equiv 0 \pmod{3^\sigma}$$

für jedes $\sigma > 2$ lösbar. Setzt man wieder

$$\eta = -2\,\xi^2 + \xi\,\Theta + \Theta^2$$
$$\eta^3 - a_1\,\eta^2 + a_2\,\eta - a_3 = 0,$$

wo

$$a_1 = 2\,(z - 3\,\xi^2)$$
$$a_2 = (3\,\xi^2 - z)^2 + 3\,\xi\,(\xi^3 - z\,\xi - x)$$
$$a_3 = (\xi^3 - z\,\xi - x)^2 - 3\,\xi\,(3\,\xi^2 - z)\,(\xi^3 - z\,\xi - x)$$

und wo die Identität besteht

$$27\,(\xi^3 - z\,\xi - x)\,(\xi^3 - z\,\xi + x) =$$
$$x^2\,\mathfrak{D} + (3\,\xi^2 - z)^3 - 3\,z\,(3\,\xi^2 - z)^2,$$

aus der folgt, dass

$$\xi^3 - z\,\xi - x \equiv 0 \pmod{3^\sigma},$$

so ist

$$\frac{\eta}{3^\sigma}$$

eine ganze Zahl, und 3 geht, wie früher gezeigt worden ist, nicht in λ auf.

Gesamtresultat für b:

Ist $z \equiv 3 \pmod 9$, so ist, wenn y durch 9, nicht durch 27 teilbar ist, 3 immer in λ enthalten und zwar einfach, wenn

$$x \equiv \pm 2 \pmod 9$$

und zweifach, wenn

$$\left.\begin{array}{l} x \equiv \pm 1 \\ x \equiv \pm 4 \end{array}\right\} \bmod 9$$

oder

Ist y durch 3^σ teilbar, wo $\sigma > 2$, so geht 3 nicht in λ auf.

c. $z \equiv 6 \pmod 9$.

In allen diesen Fällen ist y nur durch 3 teilbar.

Ist $$x \equiv \pm 4 \pmod 9,$$
so ist die Zahl
$$\eta = \frac{\Theta^2 \pm \Theta + 1}{3}$$
ganz, denn
$$S(\eta) = \frac{3 + 2z}{3}$$
ist rational und ganz,
$$S(\eta^2) = \frac{z^2 + 3z - 3(\pm x - 1)}{9}$$
ist rational und ganz, und
$$N(\eta) = \frac{(\pm x + 1 + z)(\pm x + 1) + z^2}{27}$$
ist rational und ganz.

Ist also
$$x \equiv \pm 4 \pmod 9,$$
so geht 3 nicht in λ auf.

In den beiden Fällen
$$\left.\begin{array}{l} x \equiv \pm 1 \\ x \equiv \pm 2 \end{array}\right\} \bmod 9$$
ist die Zahl
$$\eta = \frac{\alpha + \beta\Theta + \gamma\Theta^2}{3}$$
nur ganz, wenn $\alpha \equiv 0$, $\beta \equiv 0$, $\gamma \equiv 0$ ist. In diesen beiden Fällen geht 3 einfach in λ auf.

Gesamtresultat für c:

Ist
$$z \equiv 6 \pmod 9,$$
so geht 3 in λ einfach auf, wenn

$$\left.\begin{array}{rl} & x \equiv \pm 1 \\ \text{oder} & x \equiv \pm 2 \end{array}\right\} \text{mod } 9.$$

Für die Primzahl 3 ergibt sich als Endresultat:

I. 3 ist in λ einfach aufzunehmen

1. wenn y durch 3 teilbar ist, nicht durch 9, in den Fällen

$$\alpha) \quad \left.\begin{array}{l} x \equiv 0 \\ z \equiv 0 \end{array}\right\} \text{mod } 3$$

$$\beta) \quad \left.\begin{array}{rl} & z \equiv 0 \\ & x \equiv \pm 2 \\ \text{oder} & x \equiv \pm 4 \end{array}\right\} \text{mod } 9$$

$$\gamma) \quad \left.\begin{array}{l} z \equiv 6 \\ x \equiv \pm 1 \\ x \equiv \pm 2 \end{array}\right\} \text{mod } 9$$

2. wenn y durch 9 teilbar ist, nicht durch 27, in den Fällen:

$$\left.\begin{array}{l} z \equiv 3 \\ x \equiv \pm 2 \end{array}\right\} \text{mod } 9$$

II. 3 ist in λ zweifach aufzunehmen:

1. wenn y durch 9 teilbar ist, nicht durch 27, in den Fällen:

$$\alpha) \quad \begin{array}{l} z \equiv 0 \pmod 9 \\ x \equiv 0 \pmod 3 \end{array}$$

$$\beta) \quad \left.\begin{array}{l} z \equiv 3 \\ x \equiv \pm 1 \end{array}\right\} \text{mod } 9$$

$$\gamma) \quad \left.\begin{array}{l} z \equiv 3 \\ x \equiv \pm 4 \end{array}\right\} \text{mod } 9$$

2. wenn y durch 27 teilbar ist, nicht durch 81, in dem Fall

$$\left.\begin{array}{l} x \equiv 0 \\ z \equiv 0 \end{array}\right\} \bmod 9.$$

Beispiele:

Wir werden die gewonnenen Resultate noch an einigen Beispielen erläutern.

1. Als erstes Beispiel behandeln wir den Fall, dass $z = 0$ ist, und der Körper durch die Gleichung definiert wird

$$\Theta^3 = x$$

die Diskriminante dieser Gleichung ist

$$y^2 . \mathfrak{D} = \varkappa^2 . \lambda^2 . \mathfrak{D} = -27\, x^2$$

Hier ergeben sich die folgenden einfachen Resultate:

α) Die Primzahl $p > 3$ ist in λ enthalten und zwar einfach, wenn p in x aufgeht.

β) Die Primzahl 2 ist in λ aufzunehmen, wenn x gerade ist.

γ) Die Primzahl 3 geht in λ einfach auf, wenn

$$\left.\begin{array}{r} x \equiv \pm 2 \\ \text{oder} \quad x \equiv \pm 4 \end{array}\right\} \bmod 9$$

ist, und die Primzahl 3 geht in λ zweifach auf, wenn x durch 3 teilbar ist.

2. Wir untersuchen zweitens das von Woronoj behandelte Beispiel:

$$\Theta^3 + 33\,\Theta - 47 = 0$$

$$y^2 . \mathfrak{D} = 4\, z^3 - 27\, x^2 = -4 . 33^3 - 27 . 47^2$$

$$= -203391 = -3^8 . 31.$$

y ist durch $3^\sigma = 3^4$ teilbar.

Da $\sigma > 3$ ist, so geht 3 nicht in λ auf. Also ist die Körperdiskriminante

$$\Delta = -31$$

Dieses Resultat stimmt mit dem von Woronoj gefundenen überein.

3) $$\theta^3 - 49\,\theta - 196 = 0$$

$$\begin{aligned} y^2\,\mathfrak{D} &= 4\,z^3 - 27\,x^2 \\ &= 4 \,.\, 49^3 - 27 \,.\, 196^2 \\ &= 4 \,.\, 7^6 - 27 \,.\, 2^2 \,.\, 7^4 \\ &= 4 \,.\, 7^4\,[7^2 - 27] \\ &= 2^3 \,.\, 7^4 \,.\, 11 \end{aligned}$$

y ist durch $2 \,.\, 7^2$ teilbar.

α) Die Primzahl $p = 7$.

$z = 49$ ist teilbar durch 7^2
$x = 196$ ist teilbar durch 7^2.

Also geht $p = 7$ in λ einfach auf.

β) Die Primzahl 2.

$$\left.\begin{aligned} z &= 49 \equiv 1 \\ x &= 196 \equiv 0 \end{aligned}\right\} \bmod 4$$

2 geht also nicht in λ auf.

Die Körperdiskriminante ist

$$\Delta = 7^2 \,.\, 2 \,.\, 11 = 1078.$$

4) $$\theta^3 - 21\,\theta + 88 = 0$$

$$\begin{aligned} y^2 \,.\, \mathfrak{D} &= 4\,z^3 - 27\,x^2 \\ &= 4 \,.\, 21^3 - 27 \,.\, 88^2 \\ &= 4 \,.\, 27\,(7^3 - 44^2) \\ &= -4 \,.\, 27 \,.\, 1593 = -2^2 \,.\, 3^6 \,.\, 59 \end{aligned}$$

x ist durch $2 \,.\, 3^3$ teilbar.

α) Die Primzahl 2.

$$z = 21 \equiv 1 \pmod 4$$
$$x = -88 \equiv 0 \pmod 4$$

2 geht also nicht in λ auf.

β) Die Primzahl 3.

Ist y durch 3^3 teilbar, so geht 3 nur dann in λ auf, wenn

$$\left.\begin{matrix} z \equiv 0 \\ x \equiv 0 \end{matrix}\right\} \bmod 9$$

ist. Da aber

$$\left.\begin{matrix} z = 21 \text{ nicht} \equiv 0 \\ x = -88 \text{ nicht} \equiv 0 \end{matrix}\right\} \bmod 9,$$

so geht 3 in unserem Falle nicht in λ auf. Die Körperdiskriminante ist

$$\Delta = -59.$$

Lebenslauf.

Am 22. Juni 1883 wurde ich, Wanda Braun, als die Tochter des jetzigen Oberzollinspektors Braun, zu Strassburg i. Els. geboren. Ich besuchte die Müry'sche höhere Mädchenschule und die städtische höhere Mädchenschule, bestand 1902 die höhere Lehrerinnenprüfung, 1903 die Turnlehrerinnenprüfung, 1905 das Abiturientenexamen am Realgymnasium in Aachen. Seit 1905 studiere ich an der Universität Strassburg Mathematik und Naturwissenschaften. Ich hörte Vorlesungen bei den Herren Professoren Weber, Reye, Schur, Wellstein, Timerding, Epstein, Braun, Cohn, Thiele. Allen meinen Lehrern bin ich zu grossem Dank verpflichtet, ganz besonders aber meinem hochverehrten Lehrer, Herrn Professor Heinrich Weber, der mich zu dieser Arbeit anregte und mich bei Abfassung derselben mit seinem Rat stets bereitwilligst unterstützte. Auch an dieser Stelle spreche ich ihm meinen tiefgefühlten Dank aus.

Chant

G.E. STECHERT
& Co.
NEW YORK


UNIVERSITY OF ILLINOIS-URBANA
3 0112 001774055